Network Security in Software defined Networks (SDN)

Neetu Faujdar
Amity School of Engineering and Technology
Amity University
Noida, India
neetu.faujdar@gmail.com

Aparna Sinha
Amity School of Engineering and Technology
Amity University
Noida, India
aparna.sinha710@gmail.com

Harsh Sharma
Amity School of Engineering and Technology
Amity University
Noida, India
sharma.harsh3107@gmail.com

Eshaan Verma
Amity School of Engineering and Technology
Amity University
Noida, India
eshaanverma37@gmail.com

Abstract— **Based on the generalized definition of a network, we know that it is made up of a number of nodes. Sending and receiving of data takes place via these nodes. This process is characterized by the permission provided and requirement of sharing data. Basically, networking helps the nodes across the globe to connect and enable data transfer. Software Defined Networking (SDN) is a smart networking technique. It brings together other disciplines with networking for example, programming, research etc. The SDN model is predominantly controlled by a central unit called controller. All the communication takes place via this controller; however, it has a disadvantage. If the controller anyhow fails or is hacked, the entire system will either fail or get corrupted. In this paper disadvantage of the SDN has overcome with the relevant solution.**

Keywords—: Network Security, SDN, Controller

I. INTRODUCTION

In today's time, the concept of networking is becoming complicated. One must have the enormous knowledge of the networks at low and high level to get to know about the required system, working and security of network so that the complications of network can be minimized.
A Network is not only about one discipline but it also involves the multiple disciplines of programming languages like Operating Systems, Database Management System.

A network is the combination of multiple nodes. These nodes send and receive data based on the permissions and requirements.

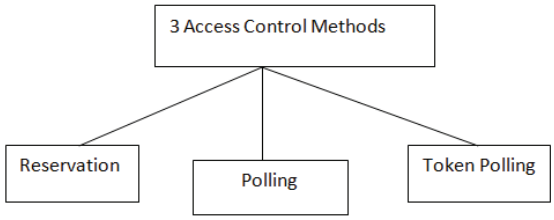

Figure 1. Access control methods

Software defined network allows the insertion of a network that manages the network through a centralized network. For the networks to advance and grow, the networking must be interrelated to various other fields of technology such as programming languages, distributed systems, operated systems, and database research. In SDN, a controller ravel is introduced which utilizes a standard relational database format and manipulates the network [6].

However, network security is still an issue and ravel is no exception. Network administration and management can be increased by bringing abstraction into play. Abstraction is basically hiding of data and displaying only the necessary data to the users. This can be done by connecting each component of the network to the centralized controller i.e. ravel which in turn reduces switches.

In Figure 2 Reservation strategy, a station needs to reserve a spot before sending information. The stations which have held their spaces move their casings in a specific order. In the event that there are N stations in the framework, there are actually N reservation smaller than usual spaces in the booking outline. After information transmission period, next reservation interim starts. Since each station realizes who will move straightaway so there won't be any collisions.

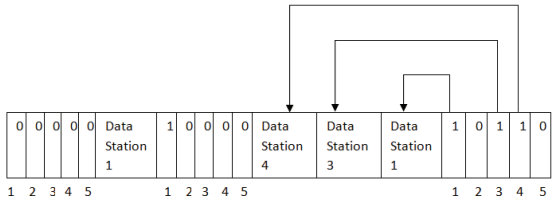

Figure 2. Reservation

In Figure 3 Polling Process, there are two types of stations, Primary Stations and Secondary Stations. The Primary Station acts a Controller that will exchange data with

Secondary Stations. Problems embody high overhead of the polling messages and high dependence on the dependability of the controller.

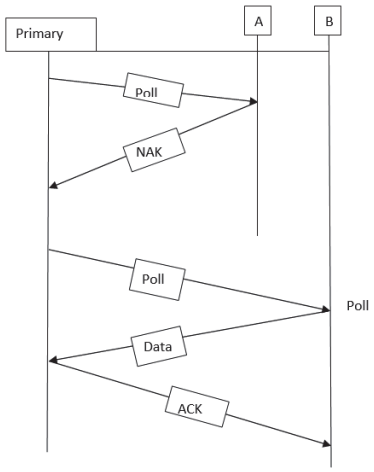

Figure 3. Polling

In Figure 4 Token Passing Method, the stations in the system are associated as a consistent ring. In this technique, an extraordinary parcel called Token courses through the ring. The ownership of the token gives the station the privilege to get to the channel and sends its information. Issues associated with this technique are duplication of token or token is lost and these issues should be handled for the right activity of this strategy.

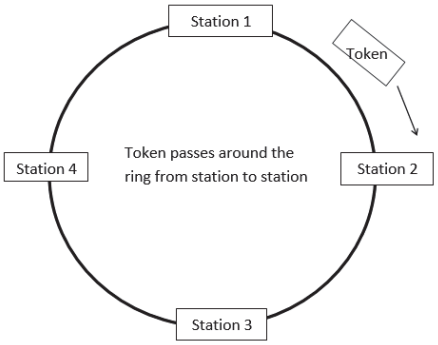

Figure 4. Token Passing

For managing SDN, use of ravel as the centralized controller and concept of abstraction are clubbed together. Ravel uses the concept of representing data using standard relational database and is therefore known as database defined controller [14]. By using ravel as a controller supports abstraction, as data can be edited, filtered, and tailored according to the needs of each controller application, essentially serving as an interface or communication protocol between the application and the controller.

It is basically a contract between the controller and the application, such that if the application wants the designated output in a format, so the controller is intended to give it in that format only. Ravel can also modify the network and coordinate the network by using SQL. All this is done by using PostgreSQL interface.

Security has always been a concern in networking which can't be compromise[7].System design was created in a period when attacks were not unmistakable but rather as the time cruised by, attacks ended up basic which brought forth numerous gadgets. Some of them are routers ACL's, firewalls, NAT's, and other center boxes notwithstanding VLANS [15]. At the point when an ACL is designed to a system, it checks the criteria of the information set up by the client and afterward chooses whether to allow or forbid the information to stream.

The function of firewall is also the similar. It is a network security that monitors and manages the incoming and outgoing data traffic based on previously set network protocols and security grounds. It establishes a barrier between trusted internal network and internet which is untrusted and contains lots of malware and attackers [13]. With the assistance of SDN organizing, administrators can utilize transfer speed the board to have support free video viewing and ideal perusing knowledge. This SDN application can likewise keep track the data transfer capacity needs at that point arrangement client streams to coordinate the idleness and transmission capacity prerequisites of the layer 7 application. This sort of use product way to deal with transfer speed the board can help in better involvement through surfing. At this phase in game, there is no uncertainty that SDN is turning into a reality in arrange. Its advantages are improved operational productivity, quicker time to showcase and new revenue in market [8].

The advanced virtualization ecosystem underpins explicit virtual assistance that is running inside the system layer. It implies a joining capacity like NFV into SDN stages [9]. It means creating an environment which is risk free and responds to the happenings very quickly. Whenever any attack occurs, every second is critical to stop the attack. It is likewise essential to examine the attack and whether different networks are shielded from it or not. SDN helps in hiding one of the most essential layers within the data centre that is network.

If there is a lot of traffic going through the network, then there is a need of a solid network and intelligence layer. Indeed, even enhancement, alarming, hypervisor mix, port arrangements, and traffic stream can be fused into system checking and knowledge advancements. Additionally, these kinds of nimble frameworks will likewise assist you with monitoring system traffic between your cloud environment and your server farm [10].

II. Related Work

In this research paper, we have focused on security related issues of software defined network. We have been studying trends of security related issues which were raised by other authors in their research papers. Therefore, this section includes the related work of other authors.

Sandra Scott-Hayward et al in their paper [1].The software defined networking can be used to increase the network security via monitoring network, analysis and its response system to various actions [11].Central controller is the highlight which is used for this process. Data which is generated and analysed by process such as traffic analysis and irregularity detection is then sent to the central controller. At the central controller, the applications are passed for the analysis and for further monitoring of data. And after the analysis, the updated rules and protocols are defined and are transferred across the network. This concept can be used to boost the speed and efficiency of the network.

Olivier FLAUZAC et al (2015) [2] presented a new SDN related architecture for networking called an SDN domain. Wire, wireless and ad-hoc networks are the components of a single domain in this system. They have also included sensor networks in their system. Next thing what they have done is basically, they have connected multiple domains with the idea of giving security resistance to each domain. After all these three conditions me, they introduced a new architecture for internet of things which is very secure and hassle free.

Changhonyoon et al. in their research paper have tried to merge different SDN features and the security related problems. Their objective is to provide these different features with proper security and management. Furthermore, the have emphasized on the fact that how many problems can arise due to this merging of security and SDN applications and how they can rectify it. To prove their research, they got to a point that their floodlight applications in real testbeds which includes switches which has SDN technology and physical hosts [3-4].

There were a lot of vulnerabilities which were due to conventional; stream of internet which was criticized by some people. Therefore, to reduce these vulnerabilities, a few security measures were undertaken to upgrade the current internet engineering. Now, these methodologies had their disadvantages too such as absence of whole control and mechanization. In this paper by Adel Zaalouk, these downsides and solutions of these downsides are discussed. To address these lacks, a few design necessities are determined to adjust the SDN engineering for security use cases [5].

III. Problem Statement

The centrally controlled SDN system is of great use as it helps to achieve the most reliable method of data transfer as per requirement. The transfer of data is also efficient and reliable. As the data is transferred from one node to another without the interference of any external node or bus architecture, so the data privacy remains intact. However, in case an external body hacks the controller, or it fails due to any reason, the entire network may crash or get corrupted. As the entire network is centrally controlled, a hold on the controller shall lead to control on the entire network. This is the main drawback of the SDN.

IV. Proposed Approach

In order to achieve a more effective and failure proof network system, two or more controllers can be used in an SDN network [12]. This will ensure that even if one of the controllers fails, the other ones will keep the system integrated and will reduce the harm caused. However, this also adds on to the complexity of the network. In this research paper, we have proposed a potential model to handle these problems.

A. The Model

Consider a simple network model of 3 nodes and 2 controllers.

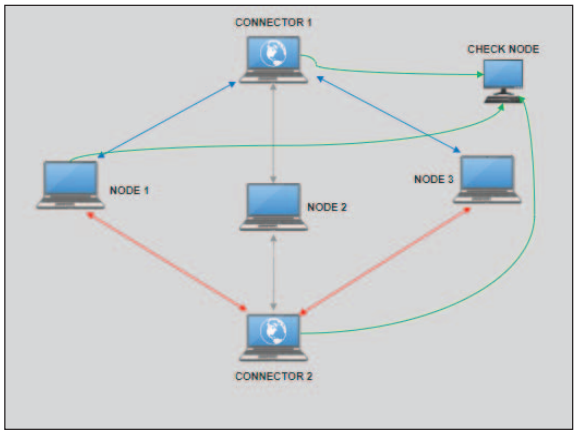

Figure 5. Model Diagram

Let us say that we have to transfer some data x from Node 1 to Node 3. Following cases can be encountered:

Case 1: Both the controller work properly without any failure.
Case 2: One of the controllers is hacked and thus fails.
Case 3: One of the controllers is hacked and data corrupted.

B. Algorithm

Step 1: Node 1 sends some data packet x to both the controller.
Step 2: Both the controllers forward the packet to the desired node (Node 3).
Step 3: Each node must receive 2 packets of data.

Case 1 : If both the packets are same, discard one of them and use the other one.
Case 2: If only one packet is received, it means that one of the controllers has failed.

However as we have received data from another controller, so the network doesn't crash and the flow of data continues. Also, with this system we get timely information about the failure which can be used to re-establish the controller.

Case 3: If both the packets received are different, then a check node gets activated, it compares the data sent by the

node with the ones forwarded by the controller.

Condition 1: If data from node matches with the data sent by controller 1, then Controller 2 is corrupt. Thus, we will discard the data from controller 2 and the one from controller 1.

Condition 2: If data from node matches with the data sent by controller 2, then controller 1 is corrupt. Thus, we will discard the data from controller 1 and the one from controller 2.

By this method, we can also deduce that which controller has been corrupted.

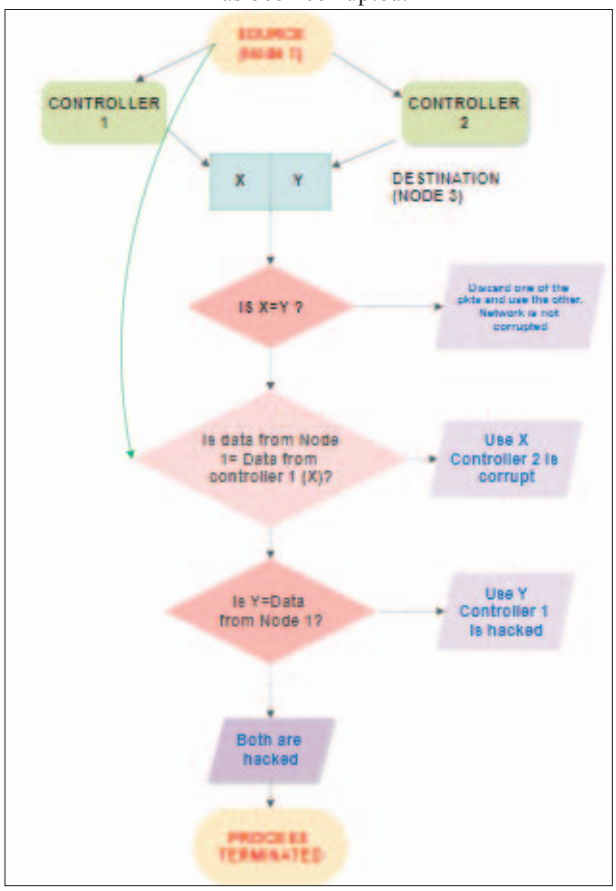

Figure 6. Algorithm

V. CONCLUSION

On the basis of the above designed algorithm, we can conclude that by using multiple controllers and check nodes, the security issues in an SDN network can be resolved. The check nodes can be created by using the concept of linking via address passing (like in case of linked list). Apart from this, we can also alert the server about the external threats on time using this algorithm. Thus this topic provides scope for future research along with providing a proposed solution.

REFERENCES

[1] SDN Security: A Survey. / Scott-Hayward, Sandra; O'Callaghan, Gemma; Sezer, Sakir. 2013 IEEE SDN for Future Networks and Services (SDN4FNS). Institute of Electrical and Electronics Engineers (IEEE), 2013. p. 1-7

[2] Olivier Flauzac, Carlos González, Abdelhak Hachani, Florent Nolot SDN based architecture for IoT and improvement of the security 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 688-693, 2015.

[3] Seungwon Shin, Lei Xu, Sungmin Hong, Guofei Gu Enhancing network through SDN 2016/8/12016 25th international conference on computer communication and networks (ICCCN)1-9.

[4] Rahamatullah Khondoker, Adel Zaalouk, Ronald Marx, Kpatcha BayarouFeature-based Comparison and Selection of SoftwareDefined Networking (SDN) Controllers2014/1/17 2014 World Congress on Computer Applications and Information Systems (WCCAIS) 1-7PublisherIEEE.

[5] Adel Zaalouk, Rahamatullah Khondoker, Ronald Marx, Kpatcha M BayarouAn orchestrator basedarchitecture for enhancing network security using SDN and network monitoring 2014/5/5ConferenceNOMSPages1-9.

[6] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh,N. McKeown, and S. Shenker. SANE: A protection architecturefor enterprise networks. In Proceedings of USENIX SecuritySymposiumVancouver, B.C., Canada, 2006.

[7] A. Nayak, A. Reimers, N. Feamster, and R. Clark. Resonance:Dynamic access control for enterprise networks. In Proceedingsof WREN, Barcelona, Spain, 20.

[8] L. E. Olson, C. A. Gunter, W. R. Cook, and M. Winslett. Implementing reflective access control in sql. In Proceedings of DBSec, Montreal, Canada, 2009.

[9] R. S. Sandhu and P. Samarati. Access control: Principles and practice. IEEE communications magazine, 32(9):40–48, Sept.1994.

[10] A. Wang, X. Mei, J. Croft, M. Caesar, and B. Godfrey. Ravel: A database-defined network. In Proceedings of SOSR, Santa Clara,CA, USA, 2011.

[11] Modieginyane, Kgotlaetsile Mathews, et al. "Software defined wireless sensor networks application opportunities for efficient network management: A survey." Computers & Electrical Engineering 66 (2018): 274-287.

[12] Zhang, Yuan, et al. "A survey on software defined networking with multiple controllers." Journal of Network and Computer Applications 103 (2018): 101-118.

[13] Cabaj, Krzysztof, Marcin Gregorczyk, and Wojciech Mazurczyk. "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics." Computers & Electrical Engineering 66 (2018): 353-368.

[14] Hu, Tao, et al. "Multi-controller based software-defined networking: A survey." IEEE Access 6 (2018): 15980-15996.

[15] Wang, K., Yin, H., Quan, W., & Min, G. (2018). Enabling collaborative edge computing for software defined vehicular networks. IEEE Network, 32(5), 112-1